



U.S. Department of Justice

*United States Attorney
Eastern District of New York*

SDD:DMP

*271 Cadman Plaza East
Brooklyn, New York 11201*

December 9, 2016

By Hand Delivery and ECF

The Honorable Brian M. Cogan
United States District Court
Eastern District of New York
225 Cadman Plaza East
Brooklyn, New York 11201

Re: Nouredine Malki v. United States
Miscellaneous Docket No. 16-1680 (BMC)
(Related to Criminal Docket Nos. 05-845, 06-216)

Dear Judge Cogan:

The government respectfully submits this letter to respond to the Court's October 8, 2016 Memorandum Decision and Order (the "Decision"), and, in light of the information set forth below, to request the Court to reconsider its ruling.

In the Decision, the Court ordered that the government either return the petitioner's laptop computer, sanitized of classified information and contraband content, within 30 days or advise the Court how long the government would need to do so. Following the Court's ruling, the government discussed the Court's ruling with the 82nd Airborne Division of the United States Army, which is the creator and original classifying authority with respect to the classified material contained on the laptop. Based on those discussions, the government offers the following response to the Court's Order.

The government agrees with the legal analysis set forth by the Court with respect to the return of property, and agrees that the appropriate issue is whether the laptop is contraband. However, the government wishes to bring additional information to the Court's attention with respect to two factual issues raised by the Decision as to whether the laptop is contraband.

First, the Court drew a distinction between the act of placing a disc containing classified information into a laptop (in which the classified information is contained only on the disc) and placing classified information onto the laptop itself. In discussing this issue with the 82nd Airborne Division, as well as with forensic computer examiners from the FBI,

the government was advised that when material from a disc is viewed on a laptop, the computer will use available memory on the physical laptop itself to open and display the file, meaning that the classified material will occupy some space on the physical laptop.¹ Here, there does not appear to be any dispute that the petitioner put a CD containing classified information into his laptop and viewed that classified information on the laptop. Accordingly, classified information may exist in portions of the physical laptop.

Second, the Court observed that merely because there was a “data spill” on the laptop cannot mean that the laptop will forever be classified as contraband. Specifically, the Court relied on Department of Defense (“DOD”) Manual 5200.01-V3 and a Committee of National Security Systems (“CNSS”) policy cited in that Manual. The government had brought the DOD Manual to the Court’s attention in support of the fact that when there is a data spill, such that classified information is “spilled” onto an unclassified medium, the unclassified medium will then become classified at the level of the classified information that was spilled. The CNSS policy cited by the Court (CNSS Policy 18) states that government agencies will “establish policies and procedures for handling classified information spillage,” leading the Court to conclude that the spill on the petitioner’s laptop could be mitigated through sanitization procedures.

In speaking with the 82nd Airborne Division, the government was advised that the sanitization procedures are designed for when there is an accidental spill of classified information onto an unclassified information system (or of higher-level classified information onto a lower-level classified system, such as a spill of Top Secret information onto an information system classified only at the Secret level), whether that information system is a government, contractor or privately owned system. The procedures are not designed to apply to the scenario where, as here, an individual steals classified information. In this case, the petitioner was convicted of, among other crimes, the willful and unauthorized possession and retention of classified information.

Nevertheless, the government requested that the 82nd Airborne Division provide the government with its procedures for handling classified information spillage in a case such as this one. As an initial matter, the 82nd Airborne re-reviewed the classified material contained on the CD recovered from the petitioner, and determined that portions of those documents remain classified today. The 82nd Airborne Division provided the attached memorandum advising that, in a situation such as the one at issue here, the appropriate sanitization procedure is the “physical or electromagnetic destruction (degaussing) of all electronic information storage volumes associated with the device.”

¹ To the extent the Court wishes to receive an evidentiary showing on this issue, the government will submit declarations from appropriate individuals. However, in light of the fact that the Court already granted the government one extension to submit this letter, the government did not want to further delay its submission in order to obtain such declarations for submission with this letter.

The Court's ruling clearly envisions that the application of sanitization procedures will result in the return to the petitioner of the laptop and non-contraband content contained on the laptop. Since the sanitization procedure set forth above would destroy all electronic information contained on the petitioner's laptop, the government thought it appropriate to advise the Court prior to taking such action.

In light of this information, the government respectfully requests that the Court reconsider its ruling, and permit the government to maintain permanent possession of the laptop, as set forth in the attached memorandum. See Paragraph 4 ("Any privately owned device involved in a spillage event will also be considered classified at the level of the classified information processed and will therefore become property of United States Government, the United States Army, 82nd Airborne Division."). In the alternative, the government can undertake the sanitization procedures set forth above, which would result in the destruction of all evidence on the laptop, and then return the laptop to the petitioner.

Respectfully submitted,

ROBERT L. CAPERS
United States Attorney

By: /s/
Douglas M. Pravda
Assistant U.S. Attorney
(718) 254-6268

cc: Clerk of the Court (BMC) (by ECF)
Noureddine Malki, pro se petitioner (by First Class Mail)



DEPARTMENT OF THE ARMY
HEADQUARTERS 82nd AIRBORNE DIVISION
2175 REILLY ROAD, STOP A
FORT BRAGG, NORTH CAROLINA 28310-5000

REPLY TO
ATTENTION OF


AFVC-GBS-SO

23 November 2016

MEMORANDUM FOR RECORD

SUBJECT: Clarification on 82nd Airborne Division G2 Policy on Sanitization Procedures resulting from Spillage Events.

1. In the event that classified information is processed in any way on a system that is not approved to process such information (henceforth "spillage"), that system will automatically be considered classified at the level of the classified information processed in accordance with DoDM 5200.01, V3.
2. The system on which the spillage occurred will be quarantined (removed from its network), if it is a networked device, and sanitized by means of the physical or electromagnetic destruction (degaussing) of all electronic information storage volumes associated with the device.
3. In the event that it is determined that the device will not leave control of the 82nd Airborne Division and that it may be re-used, the G6 may approve for the purging and validation of the device in accordance with IA BBP 03-PE-O-0003.
4. Any privately owned device involved in a spillage event will also be considered classified at the level of the classified information processed and will therefore become property of United States Government, the United States Army, 82nd Airborne Division. Classified information and classified information processing systems may not be privately owned and will be subject to the same destruction requirements.
5. The point of contact for this action is CPT Nathan S. Batesel at [REDACTED] or [REDACTED].


NATHAN S. BATESEL
CPT, MI
82ND Airborne Division SSO